NATIONAL STRATEGIC COMPUTING RESERVE: A BLUEPRINT

A report by the

SUBCOMMITTEE ON NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT

COMMITTEE ON SCIENCE AND TECHNOLOGY ENTERPRISE

and the

SUBCOMMITTEE ON FUTURE ADVANCED COMPUTING ECOSYSTEM

COMMITTEE ON TECHNOLOGY

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

October 2021

About the National Science and Technology Council

Established by Executive Order on November 23, 1993, the National Science and Technology Council (NSTC) coordinates science and technology (S&T) policy across the Federal research and development (R&D) agencies. Chaired by the President, the membership of the Cabinet-level National Science and Technology Council includes the Vice President, Director of the Office of Science and Technology Policy, and Cabinet Secretaries and Agency Heads with significant S&T responsibilities. A primary objective of the NSTC is to establish clear national goals for Federal S&T investments in a broad array of areas spanning virtually all the mission areas of the Executive Branch. The NSTC prepares R&D strategies that are coordinated across agencies to ensure that the Federal Government's investment packages and policies are smart and aimed at accomplishing multiple national goals. For more information see http://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

Congress established the White House Office of Science and Technology Policy (OSTP) in 1976 to advise the President and others within the Executive Office of the President on scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, and the environment. OSTP leads efforts across the Federal Government to develop and implement sound science and technology policies, plans, programs, and budgets, and it works with the private and philanthropic sectors; state, local, tribal, and territorial governments; the research and academic communities; and other nations toward this end. OSTP also assists the Office of Management and Budget with its annual review and analysis of Federal R&D in budgets. OSTP's Senate-confirmed Director co-chairs the President's Council of Advisors on Science and Technology and supports the NSTC. For more information see http://www.whitehouse.gov/ostp.

About the Subcommittee on Future Advanced Computing Ecosystem

The NSTC Subcommittee on Future Advanced Computing Ecosystem (FACE) coordinates Federal agency activities to pioneer, sustain, and enhance the advanced computing ecosystem necessary for U.S. scientific, technological, and economic leadership. The FACE Subcommittee is guided by the objectives, priorities, and recommendations outlined in the 2019 NSTC report, *National Strategic Computing Initiative: Pioneering the Future of Computing*, in alignment with the NITRD Subcommittee and other Subcommittees as appropriate.

About the Subcommittee on Networking & Information Technology Research and Development

The Networking and Information Technology Research and Development (NITRD) Program is the Nation's primary source of federally funded work on pioneering information technologies (IT) in computing, networking, and software. The NITRD Subcommittee of the NSTC Committee on Science and Technology Enterprise guides the multiagency NITRD Program in its work to provide the R&D foundations for ensuring continued U.S. technological leadership and meeting the needs of the Nation for advanced IT. The National Coordination Office (NCO) supports the NITRD Subcommittee and the Interagency Working Groups (IWGs) that report to it. For more information see https://www.nitrd.gov/about/.

About this Document

This report outlines a Federal proposal for setting up a National Strategic Computing Reserve (NSCR) that can be called on in times of national crisis to rapidly activate a multisector advanced computing reserve infrastructure that can speed solutions, and it defines a blueprint for operational and coordination structures that will support an NSCR implementation. The formation of the NSCR suggested in this document is based on the U.S. experience in 2020 of initiating and operating the COVID-19 High Performance Computing Consortium and a public Request for Information on Potential Concepts and Approaches for an NSCR.

Copyright Information

Published in the United States of America, 2021.

National Science and Technology Council

Chair

Eric Lander, Director, OSTP

Acting Executive Director

Kei Koizumi, OSTP

Committee on Technology
Subcommittee on Future Advanced Computing Ecosystem

Co-Chairs

Manish Parashar, Office Director, National Science Foundation (NSF) Computer and Information Science and Engineering (CISE) Directorate, Office of Advanced Cyberinfrastructure (OAC)

Steve Binkley, Principal Deputy Director, Department of Energy Office of Science (DOE/SC)

Amy Friedlander, NSF/CISE/OAC

Erwin Gianchandani, Senior Advisor for Translation, Innovation, and Partnerships, NSF

Zachary Goldstein, CIO and Director of High Performance Computing Consortium (HPCC), National Oceanic and Atmospheric Administration (NOAA)

Barbara Helland, Assistant Director, DOE/SC

Frank Indiviglio, Deputy Director of HPCC, NOAA

Margaret Martonosi, Assistant Director, NSF/CISE

Irene Parker, Assistant CIO of Satellite and Information Service, NOAA

Kathleen (Kamie) Roberts, OSTP/NITRD

Executive Secretary

Ji Hyun Lee, NCO/NITRD

Committee on Science & Technology Enterprise
Subcommittee on Networking & Information Technology (NITRD) Research & Development

Co-Chairs

Kamie Roberts, Director, NITRD National Coordination Office (NCO)

Margaret Martonosi, Assistant Director, National Science Foundation CISE Directorate

Executive Secretary

Nekeia Butler, NCO/NITRD

Writing Team

Manish Parashar, NSF/CISE/OAC

Amy Friedlander, NSF/CISE/OAC

Barbara Helland, DOE/SC

Erwin Gianchandani, NSF

Frank Indiviglio, NOAA

Margaret Martonosi, NSF/CISE

Raju Namburu, Department of Defense, Office of the Secretary of Defense (DOD/OSD)

Kamie Roberts, NCO/NITRD

Table of Contents

NATIONAL STRATEGIC COMPUTING RESERVE: A BLUEPRINT

Computing is playing an increasingly central role in all aspects of science and society, enabling new science and engineering (S&E) discoveries and innovations, and ensuring the Nation's health, defense capabilities, and economic competitiveness. This was evident with the mobilization of computing resources through the COVID-19 High Performance Computing (HPC) Consortium, an innovative public-private partnership that is helping to address a national and global pandemic emergency. Based on this experience as well as a recent Request for Information (RFI), this paper articulates a blueprint for a National Strategic Computing Reserve (NSCR) that could be accessed during any emergency. Such a strategic reserve, like other reserve capabilities, would deepen the Nation's resilience and, as appropriate, allow research expertise to be quickly brought to bear at critical junctures.

Background and Context

For decades, computing has played an essential role in the Nation's response to emergencies, including hurricanes, earthquakes, and wildfires, and now, a global pandemic. This essential role of computing in responding to emergencies has been particularly illustrated during the COVID-19 pandemic with the contributions and impact of the COVID-19 HPC Consortium.[1] The Consortium is making available computational resources and expertise from government, academia, nonprofits/foundations, and industry to the broader S&E community in an agile and expedient way to support research and development (R&D) related to the novel coronavirus. Computing provided by the Consortium has supported over 100 projects that have in turn allowed researchers to understand the structure of the SARS-CoV-2 virus and how it spreads, develop therapeutics and vaccinations, identify approaches to manage and mitigate its impacts, and plan and execute logistics responses such as delivery of medical supplies. Since its creation in March 2020, the Consortium has grown organically, attracting growing numbers of research proposals as well as additional resource and service providers, including international providers. Currently, the Consortium includes 43 members from all sectors and many nations, with an aggregate computing power of over 600 petaflops.[2]

The positive outcomes and lessons learned from the COVID-19 HPC Consortium led to the conceptualization of the National Strategic Computing Reserve, envisioned as a coalition of experts and resource providers that can be mobilized quickly to provide critical computational resources—including compute resources, software, data, and technical expertise—in times of national or international urgent need.

The White House Office of Science and Technology Policy (OSTP), through the National Science and Technology Council (NSTC) Subcommittees on the Future Advanced Computing Ecosystem (FACE) and Networking and Information Technology Research and Development (NITRD), issued an RFI in December 2020 to solicit community inputs to help inform potential attributes of

[1] https://covid19-hpc-consortium.org/

[2] 10^{15} floating-point operations per second.

an NSCR.[3] This report provides details and lessons learned from the COVID-19 HPC Consortium and incorporates responses to this RFI to outline a blueprint for establishing such a capability.

Lessons Learned: Experiences and Insights from the COVID-19 HPC Consortium

The COVID-19 HPC Consortium offers an example of how the computing community can collaborate to deliver scientific insights and practical innovations on an extraordinarily accelerated timeline. The Consortium brought together the Federal Government, industry, and academic leaders with international partners to put the world's most powerful computational resources to work to identify means to combat the coronavirus pandemic. Within its first week, the Consortium established an operational framework for providing computational resources for rapid crisis response. In particular, the Consortium took advantage of the processes and tools that were in place at the National Science Foundation for managing and reviewing proposals.

The Consortium effectively:

- Worked to overcome a myriad of institutional and organizational boundaries within government, industry, and academia to create a common portal for accessing advanced computing resources and to help coalesce ad hoc and defocused efforts in smaller "consortia" around the country and throughout the world;
- Ramped up with agility to meet urgent and presumably short-term needs that could not be easily addressed within ongoing industry, government, and academic programmatic opportunities without formal partnership agreements;
- Developed review, matching, and on-boarding processes that have reviewed over 180 scientific proposals with over 100 projects running or completed with publicized results;
- Created and implemented a framework for a worldwide research community via the Consortium website, webinars, international alliances, blogs, press releases, and online postings;
- Established new groups of computing users able to utilize a variety of advanced computing and data resources effectively for crisis response; and
- Accelerated cross-disciplinary programs in both basic understanding of the virus and its host interactions and early-stage drug development, mainly within university groups, and to a more limited extent, within small companies.

Experiences with the COVID-19 HPC Consortium have shown that the existence of an advanced computing infrastructure is not sufficient on its own to address urgent computational challenges. There must also be mechanisms in place to make this infrastructure—which includes not only computing systems but also human expertise, software, and relevant data—broadly accessible for specific purposes to enable a comprehensive and effective science-based response to a national or international need.

Key lessons learned from the Consortium include:

- Leveraging existing processes speeds the ability to collaborate;
- Engaging early with the stakeholder community, particularly through prenegotiated agreements, is critical to expediting positive impacts; for example, earlier collaboration

[3] https://www.federalregister.gov/documents/2020/12/22/2020-28142/request-for-information-on-potential-concepts-and-approaches-for-a-national-strategic-computing

with the National Institutes of Health (NIH), Federal Emergency Management Agency (FEMA), Centers for Disease Control and Prevention (CDC), and the medical provider community could have significantly increased and/or advanced the Consortium's impact in the areas of patient care and epidemiology;

- Substantial time and effort are required to make resources and services available to researchers to focus on their projects; it is critical to have a standing capability to support the proposal submission and review process, as well as coordination with service providers to provide the necessary access to resources and services;
- A flexible intellectual property (IP) framework is important to ensuring potential impacts of the research. Given the absence of formal operating and partnership agreements in the Consortium and the mix of public and private computing resources, the work that the Consortium supported was confined to open, publishable activities. A lightweight framework for supporting proprietary work and associated intellectual property requirements would have improved the effectiveness and impact of the Consortium, particularly in support of private-sector work on therapeutics and patient care; and
- The Consortium model only supports fundamental research, which is inadequate for many of the most important NSCR use cases; these include therapeutics and patient care (as noted above); cybersecurity and information assurance; critical infrastructure simulation and protection; humanitarian assistance and disaster recovery; and numerous homeland security and defense-related use cases. The concept for the NSCR needs to be expanded beyond fundamental research to permit its application to these and other emergent, sensitive, and mission-critical use cases.

While the Consortium has been successful and effective, earlier coordination of priorities and reviews with NIH, FEMA, and CDC could have improved its effectiveness, particularly in the area of patient-level projects. Note that the recommendations listed above are consistent with the recently released Computing Community Consortium (CCC) Quadrennial Paper, *Pandemic Informatics: Preparation, Robustness, and Resilience*.[4]

Motivating an NSCR

The Consortium has demonstrated the essential role of computing and data analytics in addressing the coronavirus pandemic. However, its rapid creation was largely due to the ability to leverage existing investments along with the shared sense of urgency among stakeholders, which allowed for the use of ad hoc processes fine-tuned along the way. The ad hoc creation and operation of the Consortium had significant impacts on the workloads of the personnel involved as well as on the communities that are typically served by the resources that were diverted to address the pandemic. Moreover, the shift in focus of the resources to pandemic-related research delayed other S&E projects, putting on hold advances in the broader research ecosystem. As a result, there have been some potentially undesirable implications—for example, for long-term competitiveness—of diverting human and computing resources to emergency response.

Because computing and data analytics are expected to play an increasingly critical role in addressing future national emergencies, it is important to leverage the experiences of the Consortium to establish the structures and processes now that will allow the rapid mobilization of

[4] https://cra.org/ccc/wp-content/uploads/sites/2/2020/11/Pandemic-Informatics_-Preparation-Robustness-and-Resilience.pdf

resources in the future so as to maximize their effectiveness and use and to minimize detrimental side-effects such as delays to existing S&E portfolios. It is also important to ensure that the deployment and operation of these resources is coordinated with other responses to amplify their impact. The overarching goal of instituting an NSCR is to establish these structures and processes so they are readily available when they are needed.

Community Input: RFI on Potential Concepts and Approaches for an NSCR

The RFI on Potential Concepts and Approaches for a National Strategic Computing Reserve, issued by OSTP through the NSTC FACE and NITRD Subcommittees, aimed to aggregate the lessons learned from the COVID-19 HPC Consortium with other broader community input toward the potential design of an NSCR effort. Responders were asked to answer one or more of the following:

1. ***Deployment Scenarios:*** What are envisioned scenarios under which it would be beneficial to make NSCR computational resources available for use? What are relevant characteristics to consider regarding the design of triggers for activating and deactivating the NSCR? What approaches might the NSCR utilize to test readiness for such scenarios? Are there other barriers to activating an NSCR that would need to be addressed?
2. ***Computational Resources:*** By what means will the NSCR computational resources be recruited, vetted, and sustained for use when needed? What are appropriate incentives and mechanisms for compensation? What principles might be employed in assessing the suitability of resources for inclusion in the NSCR? What types of research (e.g., fundamental research, Controlled Unclassified Information research, proprietary research) should the NSCR be provisioned to support?
3. ***NSCR Providers:*** How should the resource providers' contributions to an NSCR be determined? What approaches should guide the selection and allocation of the NSCR computational resources to users, and what roles do resource providers have in determining these approaches? By what means can the NSCR computational resource providers opt in or opt out on computational resource allocations?
4. ***NSCR Users:*** By what means and with what principles should allocations for NSCR computational resources be considered? What should constitute eligibility to apply for computational resources? What kind of eligibility restrictions/selection criteria would be appropriate for users and the use cases of applications of an NSCR?
5. ***Community Formation:*** What types of community outreach and communications will help enhance the likelihood of connecting the NSCR computational resources to the relevant computational, scientific, and emergency-response communities? With what organizations and services should the NSCR coordinate to enhance its effectiveness?
6. ***Partnership Agreements:*** What are key aspects of partnership agreements (e.g., access to results, intellectual property rights) that can help sustain the NSCR over time?
7. ***Relationship to Other Strategic Reserves:*** Are there other strategic reserves that are relevant to an NSCR? How can an NSCR connect to or interface with those reserves? What lessons can be learned from other strategic reserves that might inform the process of standing up an NSCR?

The RFI closed on January 16, 2021. Seven responses were received from the following organizations and individuals:

- COVID-19 HPC Consortium Executive Committee;
- Cybersecurity and Infrastructure Security Agency;
- Hewlett Packard Enterprise;
- Immortal Machines Inc.;
- Jacob Barhak, SimTK (simtk.org);
- Lawrence Livermore National Laboratory; and
- Rensselaer Polytechnic Institute.

A summary of the responses to the RFI is included as Appendix A to this document. The NSCR vision, implementation, and operations presented below incorporates these responses and the lessons learned from the experiences and insights of the COVID-19 HPC Consortium.

The NSCR Vision

The NSCR is envisioned as a coalition of experts and resource providers (of compute, software, data, and technical expertise) spanning government, academia, nonprofits/foundations, and industry supported by appropriate coordination structures and mechanisms that can be mobilized quickly to provide critical computing capabilities and services in times of urgent need.

This NSCR vision is analogous to the roles of the Civil Reserve Air Fleet[5] and the United States Merchant Marine[6] (among others) that are not part of the U.S. military but can be called upon to assist the military in a crisis. The NSCR blueprint comprises volunteer subject-matter experts working with computing resource providers to make advanced computing and data resources and services available to respond to crises.

In much the same way as the Merchant Marine maintains a set of "ready reserve" civilian mariners and merchant vessels that can be put to use in wartime, the NSCR aims to maintain reserve computing capabilities that can be made available in times of urgent national need. Like the Merchant Marine, this effort involves building and maintaining sufficient infrastructure and human capabilities, and ensuring that these capabilities are organized, trained, and ready in the event they need to be activated. The principal functions of the NSCR include:

- Establishing clear policies, processes, and procedures for activating and operating the NSCR in times of crisis;
- Recruiting and sustaining a group of advanced computing and data resource and service provider members in government, industry, and academia;
- Developing relevant agreements with members, including provisions for augmented capacity and/or cost reimbursement for deployable resources, for the urgent deployment of computing and supporting resources and services, and for provision of incentives for non-emergency participation;
- Developing methods and tools for making critical proprietary datasets securely available to compute platforms and researchers when needed;
- Developing a set of agreements to enable the NSCR to collaborate with Federal agencies and industries in preparation for and execution of NSCR deployments;

[5] Civil Reserve Air Fleet – 10 U.S.C § 9511(12) Civil Reserve Air Fleet program

[6] United States Merchant Marine – 46 U.S.C. § § 861-889 Merchant Marine Act

- Executing a series of preparedness exercises with some recurring frequency to test and maintain the NSCR;
- During a crisis,
    - Executing procedures to receive project proposals and review and prioritize projects and to allocate computing resources to approved projects;
    - Tracking project progress and disseminating products (including software and data) and outputs to ensure effective use and impact; and
    - Participating in the broader national response as an active partner; and
- Following a crisis,
    - Managing the return to normal operations of the involved resources;
    - Implementing changes from post-crisis lessons learned; and
    - Documenting experiences and outcomes.

NSCR Implementation and Operation

Organizationally, the NSCR is envisioned as comprising three key *implementation* components—resource providers, users from the broad S&E community, and a program office to manage the NSCR—and five key *operations* components: defining triggers and activating the Reserve, partnerships, resource allocation and user onboarding, Reserve exercises, and oversight.

NSCR Implementation

Resource Providers

The NSCR is envisioned as providing a range of resources including computing, software, data, services, expertise, etc., with resource providers spanning government, academia, industry, and nonprofits. For example, computing resources may include HPC systems, which are typically operated by government agencies and academic institutions and may also exist at nonprofit and commercial facilities. Other examples are cloud computing systems, which are often made available by commercial providers. Similarly, interoperable software stacks are essential to support applications to be executed across the range of computing platforms. Additionally, services and expertise are required for matching requests to resources, allocating resources, and onboarding users to resources.

Data resources are critical to the success of an NSCR, and it is important to work with subject-matter data providers, Federal agencies, and other stakeholders to establish necessary data-sharing processes and policies to ensure that relevant datasets are available for exercise and training purposes as well as during crisis activations. Examples of such data include biological and medical datasets for biomedical crises, and transportation, geospatial, and observational datasets for weather or seismic emergencies. Since some critical datasets are proprietary, the NSCR will need to provide methods and tools for making these data securely available to compute platforms and researchers for use in crises.

A range of incentive and/or compensation mechanisms may be considered for resource providers. For example, in the case of federally funded resource providers participating in the NSCR, one option may be to provide funding to support up to a predetermined percentage of additional capacity when systems are deployed and to provide corresponding operational funding. This extra capacity would fill mission needs when the system is not in use for national emergencies but the NSCR will require a commitment by resource providers to provide a much larger fraction of the system and support staff for NSCR use during emergencies. Federally funded resource providers may be provided other incentives as well, to opt in and to volunteer some fraction of their resources to the NSCR in times of urgent need.

Users

NSCR users are expected to span the broad S&E community working on R&D aimed at addressing the national crisis. These users will submit proposals that outline their readiness to perform the work, their expected impact on the crisis (if successful), a list of needed provider resources, and a plan to disseminate the project results and to release to the public domain the data and code used to complete the project.

Program Office

Standing up an NSCR Program Office is recommended, to be the overarching entity responsible for operating the NSCR. The Program Office will implement the principal functions listed in the Vision section above and the principal functions detailed in the next section, NSCR Operations.

NSCR Operations

Defining Triggers and Activating the Reserve

The NSCR Program Office, working with stakeholders as well as oversight entities, will develop specific activation and deactivation criteria for anticipated future crises that benefit from the computing, data, and technical expertise resources available from the NSCR. The Program Office will also develop the required protocols and procedures, as well as a set of preliminary scenarios.

Following the defined protocols and procedures, the Program Office will initiate the “approval” process for activation of the NSCR. In addition, working with domain experts and responders, the Program Office will be able to request the oversight entities to activate the NSCR in cases that do not match preplanned criteria.

Partnerships

Developing partnerships and agreements with agencies and other researchers and stakeholders is an essential component of establishing an effective NSCR. These partnerships will be important in preparing for deployment of the NSCR as well as in real-time operations during a crisis. These partnerships will also be essential to ensuring that NSCR users have access to necessary state-of-the-art technologies, tools (e.g., modeling and data analysis software), data, and expertise.

Resource Allocation and User Onboarding

The NSCR Program Office, in consultation with the stakeholders and oversight entities, will develop policies and processes for allocation and monitoring of resources once activated. These processes should include agile and rapid “matching” processes, involving all stakeholders, to determine the appropriateness of the request and the resource(s) best suited to the request. The Program Office will also maintain a standing capability to support the proposal submission and review process as well as to coordinate with service providers to provide the necessary access to resources and services.

Recognizing the support needed during onboarding users to allocated resources and ensuring that these resources are used most effectively will be critical, as will be providing users access to subject matter experts and technical support staff.

Finally, the Program Office will collect information on the utilization of resources and services as well as ensure reporting on the outcomes of the enabled work. This information is necessary to evaluate progress and impact as well as inform how the NSCR might adjust policies or practices to improve impact.

Reserve Exercises

Having a reserve of computing capability is useful only if it can be rapidly deployed by stakeholders and resource providers during a crisis. The NSCR will need to hold periodic exercises (at least one per year) to demonstrate the readiness of the infrastructure. The training exercises will serve not only to reposition resources for use in a crisis but also to test the software tools and distributed infrastructure that will need to be activated rapidly and at scale during a crisis, and to build working relationships between computing facility expert staff and the domain experts who will use the machines in a crisis (e.g., epidemiologists, hurricane modelers, responsible agency crisis managers, etc.). These exercises should focus on a variety of potential disasters and engage appropriate stakeholders at the computing facilities, among the scientific community, and among Federal, State, local, and/or tribal authorities likely to be involved in the response to each type of crisis.

Oversight

Effective oversight of the NSCR, including its structure, policies, and operations, will be critical to its successful operation. A Federal body (separate from the Program Office) should serve as "oversight provider," responsible for ensuring coordination across agencies and for approving activation and resource allocation policies. The oversight provider will ensure that the NSCR is operated in accordance with all applicable laws and with appropriate data privacy and security policies.

A separate NSCR Advisory Board comprising selected stakeholder representatives is recommended to periodically review the operations of the NSCR and provide advice and guidance to improve its readiness for, effectiveness, and impact in crisis activations.

NSCR Cost Estimates

An initial implementation of an NSCR will require investments in the following components.

1. Establishment of a Program Office responsible for managing the operation of the reserve (including the operation and maintenance of the cyberinfrastructure [CI] platform), enforcing policies for the triggering and ramp-down of the reserve, coordinating across the stakeholders as well as with other reserves, interfacing with oversight entities, executing readiness testing exercises, engaging with subject matter experts, and providing training and outreach. Members of the Program Office staff may include individuals on detail from Federal agencies. Estimated cost: $2 million (per year).
2. Development and deployment of an integrated CI Platform to support dynamic federation of resources across the different stakeholders, on-demand allocations and provisioning of these resources, and the execution of user applications and supporting software across the federation. Estimated cost: $2 million (per year).
3. Acquisition of resources, across stakeholders, that will be provisioned by the NSCR. Initial investments should explore different models for acquiring these resources, including leveraging ongoing investments by supplementing capacity as an incentive, as well as

exploring models for reimbursement with commercial cloud providers. Experiences with similar models at agencies indicate that 20% of additional resource capacity in the steady state is necessary to ensure adequate resources for future emergencies. Estimated cost: 20% of an agency's investments in resources (per year).

Conclusion and Next Steps

As demonstrated by the effectiveness of the numerous computing-aided responses to COVID-19, advanced computing infrastructure is a strategic national asset that can serve as an important tool for crisis response. To effectively mobilize this asset in a crisis, a well-planned and well-organized program is needed.

The NSCR blueprint presented in this document draws from the experience and lessons learned from the COVID-19 HPC Consortium and from observations shared in the NSCR RFI responses of how the scientific community, Federal agencies, and healthcare professionals came together in short order to allow computing to play an critical role in addressing the COVID-19 pandemic. The blueprint provides a path for the Nation to be better prepared with an accessible strategic reserve of advanced computing resources, services, and expertise that can accelerate its response to, mitigation against, and recovery from future national emergencies, whether they are natural disasters like hurricanes, earthquakes, or wildfires; public health emergencies like pandemics; manmade or environmental disasters like chemical spills, or mission crises such as when space missions are in jeopardy. A ready strategic computing reserve can nimbly make available such tools as rapid-turnaround modeling and prediction, high-speed simulations, real-time data assimilation and analysis, geospatial analysis, scientific visualizations, infrastructure resiliency, and machine learning for in-depth decision support. Increasingly, the Nation's computing infrastructure—and ready access by experts to this infrastructure, along with critical scientific and technical support in times of crisis—is critical to the Nation's safety, security, and resiliency.

The Federal Government's next steps to building on the blueprint include establishing an interagency group to conduct deeper dives into the various structural and operational components of the NCSR outlined in this document; organizing community events to explore the NSCR's role in specific emergency scenarios; and establishing the requisite relationships with other reserves as well as other entities responsible for coordinating and responding to emergencies.

Appendix A. Summary of Responses to the Request for Information on Potential Concepts and Approaches for a National Strategic Computing Reserve (NSCR)[7]

Seven responses to the request for information had been received when it closed on January 16, 2021. These responding organizations/individuals are listed below. This appendix provides highlights from the responses to the RFI questions. The summaries of the responses include in parentheses letters that correspond to the organizations or individuals that provided input on the questions:

A. COVID-19 HPC Consortium Executive Committee
B. Cybersecurity and Infrastructure Security Agency (CISA)
C. Hewlett Packard Enterprise
D. Immortal Machines Inc.
E. Jacob Barhak, SimTK (simtk.org)
F. Lawrence Livermore National Laboratory
G. Rensselaer Polytechnic Institute

1. ***Deployment Scenarios: What are envisioned scenarios under which it would be beneficial to make NSCR computational resources available for use? What are relevant characteristics to consider regarding the design of triggers for activating and deactivating the NSCR? What approaches might the NSCR utilize to test readiness for such scenarios? Are there other barriers to activating NSCR that would need to be addressed?***

   - **Scenarios/Triggering:** Respond to emergencies, incidents, and disasters that are of a substantial magnitude (All); develop agile situation-specific triggers with priorities, and consider the level of impact (A,D,F); complement other reserves and focus on providing computing resources not obtainable otherwise (C); align, when possible, with the mission of the resource provider (C); ensure deactivation criteria are defined (A).
   - **Operations/Testing:** Define governance, operations and oversight structures, as well as an infrastructure fabric that can persist (A,C,D); establish a dedicated program office to coordinate operations (A); define clear memoranda of agreements between stakeholders (F); develop regular scenario-based exercises with metrics to test execution, where possible in alignment with other reserves (A,C).
   - **Barriers:** Impact on the regular mission of the stakeholders (C); balancing crisis operations with regular operations for various stakeholders (C); the crisis/emergency may disrupt the availability of the resources that compose the reserve (C); managing the heterogeneity of resources and resource providers (A).

2. ***Computational Resources: By what means will the NSCR computational resources be recruited, vetted, and sustained for use when needed? What are appropriate incentives and mechanisms for compensation? What principles might be employed in assessing the suitability of resources for inclusion in the NSCR? What types of research (e.g., fundamental research, Controlled Unclassified Information research, proprietary research) should the NSCR be provisioned to support?***

[7] https://www.federalregister.gov/documents/2020/12/22/2020-28142/request-for-information-on-potential-concepts-and-approaches-for-a-national-strategic-computing

- **Recruiting resources:** Use an open call with well-defined requirements, and an agile process (A,C); leverage existing consortium members (A,C); leverage existing funding mechanisms and provide incentives for participating in the reserve (A,C,F); ensure that resources recruited include software, data, networking, expertise, and training (C,G); establish different resource classes and map to different use cases and requirements (e.g., real-time, large-scale, protected, etc.) (A,C); provide access to "test" systems for development and on-ramping (E); support the evolution of the reserve and the integration of emerging systems/technologies (G).
- **Assessment of suitability:** Focus on unique capabilities provided and develop thresholds, e.g., for performance and scale (A,C,F); involve all stakeholders in selection (C); develop a unified application deployment platform across resource providers (A).
- **Research supported**: Focus on urgent, time-sensitive research (C); require the sharing of results from the research as well as associated data and software, with a possible embargo period (C); provide support for relevant proprietary research when appropriate and needed (D).

3. ***NSCR Providers: How should the resource providers' contributions to NSCR be determined? What approaches should guide the selection and allocation of the NSCR computational resources to users, and what roles do resource providers have in determining these approaches? By what means can the NSCR computational resource providers opt in or opt out on computational resource allocations?***

- **Contributions:** All providers define the type/level of their resource (compute, software/data, services, expertise) contributions based on their mission (C); establish a committee with representation from all stakeholders to determine contributions and metrics (C); ensure longer-term stability of resource providers and availability of resources (E).
- **Selection:** Leverage mechanisms established by the COVID-19 HPC Consortium (A,F); establish matching/technical committees with appropriate stakeholders (A,C,F); ensure quick on-boarding (C,F).
- **Opt-in/out:** Resources provided should not have the option to opt out of providing resources if those resources match an identified need during the operation of the reserve (C).

4. ***NSCR Users: By what means and with what principles should allocations for NSCR computational resources be considered? What should constitute eligibility to apply for computational resources? What kind of eligibility restrictions/selection criteria would be appropriate for users and the use cases of applications of NSCR?***

- **Allocations:** Leverage mechanisms established by the COVID-19 HPC Consortium (A,F); prioritize allocations based on the impact on the emergency (A,C); support relevant proprietary research when appropriate and needed, and develop mechanisms to honor intellectual property (IP) (D).
- **Eligibility/selection criteria:** Consider the readiness of the users during selection (A,C); take the nature of the emergency and ability to impact it into account during selection (A,C); consider provider constraints while selecting and mapping (A); consider the ability of the user to release results, code, and/or data to the public domain (E); there should be no restrictions on the type of users who are eligible (E).

5. ***Community Formation: What types of community outreach and communications will help enhance the likelihood of connecting the NSCR computational resources to the relevant computational, scientific, and emergency-response communities? With what organizations and services should the NSCR coordinate to enhance its effectiveness?***

    - **Outreach/Communications**: Leverage mechanisms established by the COVID-19 HPC consortium (A); proactively nurture and sustain a user community through workshops and training activities and in coordination with other reserves (A,C,D); leverage resources available at the Cybersecurity and Infrastructure Security Agency (CISA) (B).
    - **Organizations and services:** Leverage the CISA Ad Hoc Response Campaign Toolkit and Templates that allow for rapid response to incidents to engage CISA stakeholders and champion CISA resources and mitigations (B); maintain relationships with the technical community (E).

6. ***Partnership Agreements: What are key aspects of partnership agreements (e.g., access to results, intellectual property rights) that can help sustain the NSCR over time?***

    - **Partnerships:** Leverage mechanisms established by the COVID-19 HPC Consortium (A,F); maintain agility and reduce overheads and legal and IP barriers (A); leverage the standing organizations such as sector-specific councils and the Critical Infrastructure Partnership Advisory Council (B); leverage the CISA stakeholder relationship management tools to identify key stakeholders in the most relevant sectors or industries related to the incident in question (B).

7. ***Relationship to Other Strategic Reserves: Are there other strategic reserves that are relevant to NSCR? How can NSCR connect or interface with those reserves? What lessons can be learned from other strategic reserves that might inform the process of standing up a NSCR?***

    - **Relationships:** Activate the reserve in partnership with other reserves, as appropriate, based on the nature of the emergency (A); coordinate structures, governance, triggering, operations, testing, etc., and share best practices across reserves (C); explore international linkages (as in case of the COVID-19 HPC Consortium) (C).